PURPOSE
To identify standards for the authorized access and security of the Riverside County Emergency Medical Services Information System (REMSIS) for the purposes of data collection, data submission, and data analysis. REMSIS refers to the centralized EMS data system and repository to which all electronic patient care data is collected, submitted, stored, and analyzed. This policy shall apply to all cases of access and utilization of any component of REMSIS.

AUTHORITY
California Health and Safety Code - Division 2.5: Emergency Medical Services [1797. - 1799.207.]
1. Each organization submitting data to REMSIS shall retain access rights to their own data.
2. EMS Provider organizations utilizing REMSIS shall have access to their own data for the purposes of CQI, billing, statistical analysis, operational use, and data submission to REMSA.
3. Base Hospitals shall have access to and may utilize REMSIS for the provision of medical direction and CQI.
4. Hospitals accessing REMSIS shall only have access to patient care data for those patients transported to their facilities.
5. REMSA shall have access to all data submitted into REMSIS for regulatory purposes, including but not limited to: CQI, statistical analyses, and data submission to the State EMS Authority.
6. REMSA shall redirect information requests, such as subpoenas, to the applicable organization upon receiving such a request.

Types of User Permission Groups
1. User permission groups for provider organizations:
   a. **Provider** – This type of access is for field providers who will be utilizing REMSIS to complete electronic PCRs in the field. Users at this level will only be able to create and edit electronic PCRs. Examples of users at this level are the EMTs and paramedics working on an ambulance or fire apparatus.
   b. **Service reports** – This type of access is for provider organization personnel who will need access to their organization’s data for analytics. This level of access is able to run existing reports on data but may not create custom reports. This level of access will not generate electronic PCRs.
   c. **Service QA/QI** – This type of access is for provider organization personnel who will need to perform advanced or custom analytics on their organization’s data. This level of access is able to create custom reports in addition to running existing reports. This level of access may not generate electronic PCRs.
   d. **Service billing** – This type of access is for provider organization billing personnel who will need access to their organization’s data for billing purposes. This level of access is able to run existing reports on data but may not create custom reports. This level of access will not generate electronic PCRs.
   e. **Service admin** – This type of access may view all data owned by the respective organization and perform all tasks granted to the previous three levels of access. The Service Admin may also create and edit user accounts for authorized users at the Service Staff, Service Report, and Service QA/QI levels.
2. User permission groups for hospitals:
   a. **Hospital Hub user** – This type of access is for hospital staff members who may only view the hospital dashboard and print electronic PCRs for their respective facility.
   b. **Hospital Hub reports** – This type of access is for hospital staff members who need to run existing reports on patient care data for patients transported to their facility.
c. **Hospital Hub admin** – This type of access is for the designated administrator(s) at each hospital who shall create and maintain user access of the previous two types.

3. Use permission groups for training institutions:
   a. **Student** – This type of access is for currently enrolled EMS students to create demonstration electronic PCRs to facilitate an introduction to REMSIS as well as data collection during designated training periods (e.g., field or clinical internships).
   b. **Training program admin** – This type of access is designated for the administrator(s) at each training institution who shall verify student user accounts during designated enrolled training periods.

**Authorization of Access**

1. Each organization utilizing any component of REMSIS shall designate one (1) individual as the primary administrator and at least one (1) different individual as the secondary administrator for that organization. The administrators shall have access to their organization’s data and shall serve as the point of contact for REMSIS-related communications between their organization and REMSA. The administrators shall issue and maintain non-administrator access for all other personnel within their organization as appropriate.

2. REMSA shall issue and maintain administrative user access to REMSIS and will audit authorized administrative users annually, and as needed, for system QA/QI.

3. Any user found to have been inactive within REMSIS for a period exceeding 180 days shall have their access temporarily suspended until their respective organization’s administrator officially notifies REMSA that the user is still authorized to access the system.

4. Provider organization shall officially notify REMSA to initiate or terminate administrator access.

**Data Security and Privacy**

1. Each person authorized to access any portion of REMSIS shall maintain a unique password which may not be shared with any other person.

2. Each agency or organization which collects, utilizes, or transmits patient care data in any fashion shall comply with all local, State, and Federal laws pertaining to such activities, including but not limited to the Health Information Portability and Accountability Act (HIPAA) and the California Confidentiality Medical Information Act (CMIA).

3. Each agency or organization which collects, utilizes, or transmits patient care data in any fashion shall implement electronic security measures to protect the data from unauthorized access, including but not limited to the password protection and encryption of all electronic devices used to interface with REMSIS.

4. Each agency or organization which collects, utilizes, or transmits patient care data in any fashion shall implement a data security plan, including but not limited to:
   a. HIPAA and CMIA compliance procedures and policies
   b. Electronic data capture device security procedures and policies

5. All employees accessing any device connected to REMSIS shall receive initial and annual training in data security and protection of patient health information.

6. Each agency or organization utilizing any component of REMSIS shall immediately notify REMSA of any suspected or actual breach of data security or integrity. A breach includes but is not limited to:
   a. Suspected or actual unauthorized access of data systems
   b. Theft or loss of electronic or non-electronic media containing information that could lead to unauthorized access of data systems
   c. Theft or loss of electronic or non-electronic media containing protected health information as defined by HIPAA and/or CMIA
   d. Suspicious or unusual activity discovered on, in, or around hardware able to access REMSIS